UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/568,452	04/26/2006	Lim Wong	4448-40	8210

23117 7590 03/09/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
PHAN, HUY Q	
ART UNIT	**PAPER NUMBER**
2617	
MAIL DATE	**DELIVERY MODE**
03/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/568,452	WONG, LIM	
	Examiner	Art Unit	
	HUY Q. PHAN	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This Office Action is in response to Amendment filed on date: 02/11/2009.

Claims 1-17 are still pending.

Claims 13-17 are newly added.

Response to Arguments

2. Rejection Under 35 USC 112, Second Paragraph

Claims 2-3 and 8-9 have been amended, the 112 rejection is withdrawn.

Rejection Under 35 USC 102 (e)

Applicant stated that "this technique still involves only a single layer of verification. Thus, Khan lacks the second or further layer of authentication" (see RMARKS page 10). Assuming, arguendo, applicants' assertions are true, none of these features relied on by applicant are found in representative claims 1 and/or 7. Even if this language were in the claims, a "the second or further layer of authentication" can and does refer to the credit card company receiving the customer's PIN (see [0025]) and decides whether the PIN number entered is the correct one for those card details. If so the customer is considered authentic such that (subject to the amount of funds to be transferred being less than a predetermined maximum) the transaction is validated and the funds are transferred. (see [0022]). Interpreting this claim language as broadly as allowed, reads on Khan's PIN processing at the credit card company.

Applicant argued that Khan does not disclose "crosscheck" capability and "techniques for providing a further level of coding to access code data regarding security data to enter servers for services, money, and commerce transactions" (see RMARKS page 10). The examiner respectfully disagrees with the applicant's argument. Khan specifically discloses that the mobile phone network makes a call to the customer's mobile phone for requesting the PIN number (see [0022]) then verifies the customer's mobile phone number with the credit/debit cards owned ("inspects" see [0024]). Since, the credit/debit card company verifies the PIN and the credit/debit cards owned again (see [0026]), therefore the credit/debit card company of Khan is provided with "crosscheck" capability. Khan discloses that the customer buys items at the retail store and uses his/her mobile phone to enter the PIN in order to authorize the transaction (see [0017]). Since, Khan specifically suggests that "The sophisticated authentication and encryption techniques used generally in mobile telecommunications add to the security that is provided" and the PIN is requested and received by the mobile phone network before the credit/debit card company processes the PIN, therefore one of ordinary skill in the art would see that Khan suggests "techniques for providing a further level of coding to access code data regarding security data to enter servers for services, money, and commerce transactions".

Rejection Under 35 USC 103(a)

In response to the applicant's argument, with regard to the rejection of claims 2 and 8 under 35 USC § 103(a) over Khan in view of Rosenberg, it is believed that Khan discloses all the limitations of the independent claims (see section above) from which

claims 2 and 8 depend, respectively. Thus, the combination of Khan and Rosenberg can be used to establish prima facie obviousness for claims 2 and 8 because the references teach or suggest all claim limitations as required. See MPEP § 2143.03. Therefore, prima facie obviousness under 35 U.S.C. § 103 has been established.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3-7 and 9-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Khan (US 2004/0248554; previously cited).

Regarding claim 1, Khan discloses a data and mobile telephony telecommunication open virtual secure crosscheck-link communication service channel (“by dialing up a specific telephone number” see [0021]) system (fig. 3) configured to provide a further level of coding to access code data (“Personal Identification Number (PIN) number” (see [0021]) is transmitted in CDMA communication system" (see [0014]) or in encryption techniques (see [0016])) regarding security data to enter servers for services, money, and commerce transactions ([0017] and [0027]), comprising:

at least one gateway server system (“credit/debit card company's computer 306” see [0020]), having communication connecting input interfaces to at least one of hardware, firmware, and software connecting any data and telecommunication network operator ("establishes a connection to a Mobile Switching Centre (MSC) 305 of a mobile phone network 307” see [0021]);

an output communication interface (“by dialing up a specific telephone number” see [0021]) from said gateway server system connecting said data and telecommunication networks to said open secure cross-link channel system [0021];

an interface connecting subscribers to a mobile telephony device to said data and telecommunication operators (“makes a call to the customer's mobile phone 309 and a recorded voice asks” see [0022]), to said open secure cross-link channel system [0021], said subscribers devices for communication having at least one identity to access said open secure cross-link channel system [0022];

a memory space (“credit/debit card company's computer 306” (see [0020]) must have a memory) in said gateway server system for every subscriber, said memory space comprising at least all information regarding said access code data, said memory space being associated to said identity (in order for “The credit card company's computer 306 decides whether the PIN number entered is the correct one for those card details” see [0026]);

at least one point for performing said transactions by providing said access code data to said gateway server [0025];

wherein a crosscheck is performed in said gateway ("The credit card company's computer 306 decides" see [0026]), to check if data belonging to said subscriber in said memory space is correct by calling the identity [0021] and thus said mobile telephony device associated to said memory space [0026]; and

wherein if the subscriber to said identity and said crosschecked memory space data [0025], having provided said access code data [0026], the transaction at said at least one point is granted if said subscriber grants the call and thus the transaction by returning a predetermined signal via said mobile telephony device [0027].

Regarding claim 3, Khan further discloses an open secure cross-link channel according to claim 1, wherein said type of transaction is performed by a PC or other computerized device ("The credit card company's computer 306 decides" see [0026]).

Regarding claim 4, Khan further discloses an open secure cross-link channel according to claim 1, wherein said identity is the telephone number to said mobile phone or other identity uniquely identifying the called mobile phone [0021].

Regarding claim 5, Khan further discloses an open secure cross-link channel according to claim 1, wherein said memory space in addition to said access code data comprises allowed currency limit and other restricting data for ordering said services [0025].

Regarding claim 6, Khan further discloses an open secure cross-link channel according to claim 1, wherein said call belongs to at least one of the following categories voice, SMS, MMS, and data, and the call, and wherein transaction is granted by entering and transmitting the signal of a predetermined PIN code (“makes a call to the customer's mobile phone 309 and a recorded voice asks” see [0022]).

Regarding claim 7, Khan discloses a method (fig. 3) in a data and mobile telephony telecommunication system providing an open virtual secure crosscheck-link communication service channel (“by dialing up a specific telephone number” see [0021]) configured to apply a further level of coding to access code data regarding security data (“Personal Identification Number (PIN) number” (see [0021]) is transmitted in CDMA communication system" (see [0014]) or in encryption techniques (see [0016])) to enter servers for services, money, and commerce transactions ([0017]-[0027]), comprising:

having communication connecting input interfaces (“by dialing up a specific telephone number” see [0021]) to at least one gateway server system (“The credit card company’s computer 306 decides” see [0026]), to at least one of hardware, firmware, and software connecting any data and telecommunication network operator ("establishes a connection to a Mobile Switching Centre (MSC) 305 of a mobile phone network 307” see [0021]);

connecting said data and telecommunication networks to said open secure cross-link channel system through an output communication interface in said gateway server system (“by dialing up a specific telephone number” see [0021]);

connecting subscribers to mobile telephony devices to said data and telecommunication operators (“makes a call to the customer's mobile phone 309 and a recorded voice asks” see [0022]), to said open secure cross-link channel system [0021], said subscribers devices for communication having at least one identity to access said open secure cross-link channel system ([0021]-[0023) ;

storing in a memory space (“credit/debit card company's computer 306” (see [0020]) must have a memory) for every subscriber in said gateway server system, said memory space comprising at least all information regarding said access code data, said memory space being associated to said identity (in order for “The credit card company's computer 306 decides whether the PIN number entered is the correct one for those card details” see [0026]);

performing through at least one point said transactions by providing said access code data to said gateway server ([0021]-[0026]);

performing a crosscheck in said gateway (“The credit card company’s computer 306 decides” see [0026]), checking if data belonging to said subscriber in said memory space is correct by calling the identity and thus said mobile telephony device associated to said memory space ([0021]-[0026]); and

if the subscriber to said identity and said crosschecked memory space data [0026], having provided said access code data ([0021]-[0026]), the transaction at said at least one point is granted if said subscriber grants the call [0026] and thus the transaction by returning a predetermined signal via said mobile telephony device [0027].

Regarding claim 9, Khan further discloses a method according to claim 7, wherein said type of transaction is performed by a PC or other computerized device ("The credit card company's computer 306 decides" see [0026]).

Regarding claim 10, Khan further discloses a method according to claim 7, wherein said identity is the telephone number to said mobile phone or other identity uniquely identifying the called mobile phone ([0021]-[0026]).

Regarding claim 11, Khan further discloses a method according to claim 7, wherein said memory space in addition to said access code data comprises allowed currency limit and other restricting data for ordering said services [0026].

Regarding claim 12, Khan further discloses a method according to claim 7, wherein said call belongs to at least one of the following categories voice, SMS, MMS, data, and the call, and wherein the transaction is granted by entering and transmitting the signal of a predetermined PIN code ("makes a call to the customer's mobile phone 309 and a recorded voice asks" see [0022]).

Regarding claim 13, Khan further discloses the open secure cross-link channel according to claim 1, wherein the further level of coding is provided on a network (fig. 3, 305 and/or 307) separate from said servers for services, money, and commerce transactions (see [0022]).

Regarding claim 14, Khan further discloses the open secure cross-link channel according to claim 1, wherein the crosscheck-link communication service channel is configured to interface, and perform at least two levels of verification between, at least two of: said servers ("authenticate" see [0021]), bank transaction and card operators ("decides… validated" see [0026]), telecommunications operators ("inspects" see [0024]), and data communication operators ("security" see [0016]).

Regarding claim 15, Khan further discloses the open secure cross-link channel according to claim 1, wherein the further level of coding is provided between the mobile network and transaction network ("The MSC 305 sends the PIN number, and the card details (card number, expiry date) to the credit card network 306" see [0025]; note: In the CDMA mobile phone network, the transmitted data must be encoded or encrypted).

Regarding claim 16, Khan further discloses the open secure cross-link channel according to claim 1, wherein the further level of coding is provided independent of a first level of coding, the first level of coding being needed to enter servers for services, money, and commerce transactions ("The MSC 305 sends the PIN number, and the card details (card number, expiry date) to the credit card network 306" see [0025]; note: the credit card network must be provided with codes or keys in order to decode or decrypt the received data from the CDMA mobile phone network).

Regarding claim 17, Khan further discloses an open virtual secure crosscheck-link communication service channel system (fig. 3), comprising:

at least one gateway server (“credit/debit card company's computer 306” see [0020]) connected to at least one external network ("establishes a connection to a Mobile Switching Centre (MSC) 305 of a mobile phone network 307” see [0021]) used to process transactions ;

a database operably connected to said gateway server (“credit/debit card company's computer 306” (see [0020]) must have a database), the database comprising information regarding access code data for accessing the at least one said external network (sends the PIN” see [0025]), the information being associated with identities of users (in order for “The credit card company's computer 306 decides whether the PIN number entered is the correct one for those card details” see [0026]) using the secure crosscheck-link communication service channel system (“security” see [0016]); and

an interface connecting said users to said secure crosscheck-link communication service channel system (“makes a call to the customer's mobile phone 309 and a recorded voice asks for the PIN” see [0022]);

wherein at least first (“authenticate” see [0021] and/or “inspects” see [0024]) and second verifications (“decides… validated” see [0026]) are independently performed when a transaction is attempted, the first verification being preformed by an appropriate one of the at least one external network (“inspects” see [0024]),

wherein at least the second verification (“decides… validated” see [0026]) is performed by the crosscheck-link communication service channel system in connection

with the information stored in the database (see [0020] and [0026]) and a user-provided input [0023], and

wherein the transaction is approved when the at least first and second verifications are satisfied ("decides… validated" see [0026]).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khan in view of Rosenberg (US 2004/0235450; previously cited).

Regarding claim 2, Khan discloses an open secure cross-link channel according to claim 1, except wherein said type of transaction is performed by utilizing at least one of a bank card, shopping card, petrol card, and credit card together with said mobile station, wherein other card information is stored in said memory space. However in analogous art, Rosenberg teaches wherein said type of transaction is performed by utilizing a bank card, shopping card, petrol card, credit card and the like together with said mobile station ("credit card" and "mobile communication device" see [0155]-[0161]), wherein other card information is stored in said memory space ("a sufficient fund" see [0162]). Since, Khan and Rosenberg are related to the method of secure crosscheck

link communication service; therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Khan as taught by Rosenberg for purpose of increasing the security for the buyer since the transaction is required at least using the credit card and the mobile station.

Regarding claim 8, Khan discloses a method according to claim 7, wherein said type of transaction is performed by utilizing at least one of a bank card, shopping card, petrol card, and credit card together with said mobile station, said cards bearing the password, wherein other card information is stored in said memory space. However in analogous art, Rosenberg teaches wherein said type of transaction is performed by utilizing a bank card, shopping card, petrol card, credit card and the like together with said mobile station ("credit card" and "mobile communication device" see [0155]-[0161]), said cards bearing the password ("PIN number" see [0161]), wherein other card information is stored in said memory space ("a sufficient fund" see [0162]). Since, Khan and Rosenberg are related to the method of secure crosscheck link communication service; therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Khan as taught by Rosenberg for purpose of increasing the security for the buyer since the transaction is required at least using the credit card and the mobile station.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) Chetty claims “wherein the user identification information further includes a card number and an expiration date from the entity being a credit card issuer and the method further comprises downloading at least the card number to the business entity for use during the transaction being a commercial transaction.” (see specification).

b) Natsuno discloses “the credit card company's server 60A sends entry screen data for prompting the user to enter information (e.g. his/hername, age, date of birth, address, phone number, employment, annual income, password, etc.) that are needed for the credit card contract with the company A, out to the Internet 70 addressed to the mobile station 100” (see specification).

c) Sakaguchi discloses “a mobile station of an owner of the settlement card is called by the card authentication and settlement processing device and a payment processing is performed in the card authentication and settlement processing device by a password or ID number assigned to the owner, which is inputted from the called mobile station” (see specification).

6. **THIS ACTION IS MADE FINAL**.

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Huy Q Phan whose telephone number is 571-272-7924. The examiner can normally be reached on 9AM-7:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Alexander Eisen can be reached on 571-272-7687. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Huy Q Phan/
Primary (TFSA) Examiner, Art Unit 2617
Date: 03/04/2009